有限群の共役類について (有限群の研究)

伊藤, 昇

数理解析研究所講究録
200巻 1974年 1-24

有限群の共役類について*

イリノイ大 伊藤昇

§1. 有限群Gの2元a, bが共役であるとは、$\exists x \in G$ $b = x^{-1}ax$と定義される、この時.

$$G = H_1 + \cdots + H_k$$

とGは共役類に分割される. ($k = k(G)$を仮にGの類数と呼ぶ)、この時.

(イ) $g = h_1 + \cdots + h_k$, 類等式

(ロ) $1 = \frac{1}{c_1} + \cdots + \frac{1}{c_k}$, $c_i = \frac{g}{h_i}$ $(i = 1, \cdots, k)$

が成り立つ. ($h_i = |H_i|$). さて.

$$\exists i > 1,\ |h_i| = p^a \implies G = \text{not simple}$$

というのはBurnsideによる周知の結果である.

*) この原稿は伊藤先生の講演を坂内がまとめなおしたものです。内容の誤りなどがありましたら、記録者の責任です。

ここでの講演は、共役類の性質が群の構造にどのように影響していくかを調べようというわけです。[記録者注：先生がこの問題をはじめた一つの motivation は、このような問題は（いわゆる orthodox な）群論とはあまり関係がないと思われたので、逆にこの方向で何か得られたら、それが群論にとって新しい method を与えるかもしれないと考えられたからだとのことですが、結果的には最近の群論と密接に結びついてしまったとのことです。]

先ず、自明な問題として次のものが考えられる。

問 1.　k = given の時 $\max\limits_{k(G)=k} g(G)$ を求めよ。

Landau (1903) Math. Ann. 56, 671–676 により（講演ではこの証明もされたが略す）$1 = \frac{1}{x_1} + \cdots + \frac{1}{x_k}$ という式についての数論的考察だけから $g \leq k^{2^{k-1}}$ が容易に得られるが（更に Miller, Trans. A.M.S. 1920 に見られるような改良もあるが）、次の list からもわかるように、実際の存在する例との間の gap ははげしい

	existence の max.	その order
$k=5$	$G = A_5$	60
$k=6$	$G = LF(2,7)$	168

$k=7$	$G=A_6$	360	
$k=8$	$G=LF(2,11)$	660	(?)

次の問題もすぐ思いつく問題である

問 2.1. max. は simple な G でとれるか?

問 2.2. simplicity は類等式で決定されるか.

次の問題はまだ解かれていないと思われる.

(*) $(i \neq j \Rightarrow h_i \neq h_j) \Longrightarrow G = S_3$?

この partial solution として、ここでは Markel の結果 ([これは講演の時はまだ未発表であったが最近 J. Algebra 26 (1973), 69−74 に表われた]) を紹介された.

定理 (Markel) 有限群 G が (*) をみたし $G' =$ nilpotent (or $|\pi(G)| = 2$) $\Rightarrow G = S_3$

一応簡簡な証明をつけると

- $G =$ rational group. (i.e., G の $\forall \chi$: character が

rational value).

- $G/G' =$ el. abelian 2-gp.
- $G \ni x, x^{-1} \Rightarrow x \sim x^{-1}$ から $2 \mid |G|$,
- $Z(G) = 1$.
- $G =$ not nilpotent
- $x \in G$, x の order $p \Rightarrow \dfrac{N_G(\langle x \rangle)}{C_G(x)} =$ cyclic of order $p-1$

等が条件(*)から直ちに得られる. 更に $G' =$ nilpotent から、$x \in Z(G')$ をとれば、$G' \leqslant C_G(x)$ から $\dfrac{N(\langle x \rangle)}{C_G(x)}$ が G/G' の section でなければならず、このことから $p = 3$ が得られる. (i.e., $G = \{2, 3\}$-群) S を G の1つの Sylow 2-subgp. とすれば、$S \cap G' = 1$ (otherwise $S \cap G' = S_2$ of G, $S \cap G' \lhd G$, 更に $G' =$ nilp かつ $G = S \cdot G'$ から $Z(S) \cap G' \leq Z(G) = 1$ が得られ矛盾) が得られ、$S \cong G/G' \cong (2, 2, \cdots, 2)$、更に $C_G(G') \leq G'$ ($\because$ $S \cap C_G(G') \leq Z(G) = 1$), $C_G(S) = S = N_G(S)$ が得られ ($\because$ $x \in N_G(S) \cap G'$, $y \in S \Rightarrow [y, x] \in S \cap G' = 1$) Burnside の lemma から S の任意の元は S で fuse しない.
さて、$|G| = 2^a \cdot 3^b$ の元の個数を数えれば、

(イ)	identity	1
(ロ)	3-elts	$3^b - 1$

(ハ) 2 - elts $\displaystyle\sum_{x\in S^{\#}}|G:C_G(x)| \le \sum_{i=1}^{b} 3^i$

(ニ) mixed elts
y

これは $|y|\equiv 0(6)$ がすぐ得られ

Ω を mixed elts の完全代表系とすれば

$$\sum_{y\in\Omega}|G:C_G(y)| \le \sum_{i=1}^{b-1}\sum_{j=1}^{a-1} 3^i 2^j$$

が得られる．辺々加えて

$$2^a\cdot 3^b \le 1+(3^b-1)+\sum_{i=1}^{b}3^i+\Big[\sum_{i=1}^{b-1}3^i\Big]\cdot\Big[\sum_{j=1}^{a-1}2^j\Big]$$

これから

$$2^a-1 \le 3^{b-1}(3-2^a)$$

従って $a=1$．i.e., $|G|=2\cdot 3^b$ が得られる。以下 $G=S_3$ を得ることは容易である。（証終）

次の問題3もThompsonの結果．

$$f_1|f_2|\cdots|f_k \implies G：決まる \qquad (f_i=\chi_i(1))$$

が出来ていることから考えて、（ひょっとしたら）証明出来てもいいかもしれない

問題3．$h_1\le\cdots\le h_k$

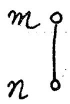
$$h_1|h_2|\cdots|h_k \implies G＝決まるか？$$

（$\Rightarrow$ 明らかに $Z(G)\ne 1$）

§2、次の話題は、Gの conjugate rank（あるいは conjugate graph）を定義して、それからGを characterize しようという試みである

定義　G:　$g = h_1 + \cdots + h_k$ に対して
$I(G) = \{n > 1,\ \exists x \in G \mid n = |G : C_G(x)|\}$ と def し
$|I(G)| = r$ をGの conjugate rank と呼ぶ
(e.g. A_5: $60 = 1 + 12 + 12 + 15 + 20$ は rank 3 である)
更に、$I(G) \ni m, n$ に対して

$$m \succ n \underset{def}{\Longleftrightarrow} m \mid n \quad \text{で}$$



という関係を入れ、出来るgraphをGの conjugate graph と呼ぶ。　なお

$$\circ \quad \circ \cdots \circ$$

というgraphを type F (free) と呼ぶ。

この問題について、今までわかっていることは次のような結果である．［ほとんどが伊藤先生の結果である］．

(1)　$\left.\begin{array}{l} r(G) = 1 \\ I(G) = \{n\} \end{array}\right) \Rightarrow n = p^a,\ \underset{p\text{-}gp}{\underset{|}{G}} = P \times \text{abelian}$
(特に $G = $ nilpotent)

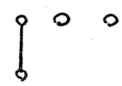
(2) $\gamma(G)=2 \Longrightarrow$ ∘ ∘ or 

 $\Rightarrow$ $G=\{p,q\}\times$ abelian (Camina)
(特に $G=$ solvable)

∘ ∘ $\Rightarrow$ $G/Z(G)$ は nontrivial partition を持つ.
この時は、Baer, Kegel, Suzuki 等による分類を用いて、$G=$ solvable がわかる。

☆  の場合から考えられることは、問3. の結果の予想として、$\underbrace{\{p_1,\cdots,p_r\}}_{\text{特殊なもの}}\times$ abelian が予想される。

(3) $\left.\begin{array}{l} G=\text{simple} \\ \gamma(G)=3 \end{array}\right\} \Longrightarrow$ (∘ ∘ ∘) かつ $G=LF(2,2^m)$
$m\geq 2$.

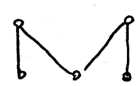
(4) $\left.\begin{array}{l} G=\text{Simple} \\ \gamma(G)=4 \end{array}\right\} \Longrightarrow$ () かつ $G=LF(2,q)$
$q=$ odd ≥ 7

(5) $\left.\begin{array}{l} G=\text{simple} \\ \gamma(G)=5 \\ \text{3-headed でない} \end{array}\right\} \Longrightarrow$ $G=S_z(q)$
or $LF(3,4)$

graph の一番上の点の数

(3-headed の場合は未解決).

さて、$\gamma(G)=6 \Rightarrow$?

この example として $LF(3,3)$ の  のような graph

がある。[なお、A_n または classical type でない単純群では $r(G) \leq 100$ であろうといわれたが、E_7, E_8 型ではもっと大きくなるとのことである。水野君他の注意]

さて、問題は、

$$\left.\begin{array}{l} r(G) = 1 \\ I(G) = n \end{array}\right\} \Rightarrow \quad G = \text{nilp}, \quad n = p^a, \quad G = P \times A$$

ということの拡張をどのように考えるべきかということであるが、これについては次の Camina の結果が目ざましい。

定理 (Camina)*)

$$\left.\begin{array}{l} G = \text{ a finite gp} \\ n = \text{ 自然数} \\ \pi = \text{ a non empty set of primes} \end{array}\right)$$ が与えられており

for $x \in G$ s.t. $\exists p \in \pi$, x は p-elt

$\Rightarrow \quad |G : C_G(x)| = 1$ or n が成り立つとする。

この時

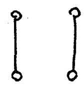
(1) $G = \text{nilp}$, $n = p^a$

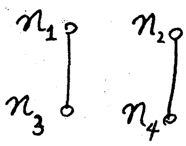
(2) $|\pi| = 1$

のいずれかが成り立つ。

*) これは、講演の時は未発表であったが、最近 J. London Math. Soc. 6(1973), 421–426 に表われた。[以下のこの証明は、伊藤先生の講演の再現よりも Camina の原論文の記録者による解読の意味あいが強い。]

例えばこの結果は次のように応用される。

応用　$\left.\begin{array}{l} r(G)=4 \\ G=\text{simple}\end{array}\right\} \Rightarrow$  でない。

応用の証明　

とおく、更に $n=n_3/n_1$ とおく。

① 先ず、$n=p^a$ (${}^\exists p=$ prime) をいう。

$\pi=\{\text{prime } q \mid {}^\exists q\text{-power elt whose centralizer is } A\}$

とおく。この時、t を $(|t|,\pi)=1$ となる A の任意の元とすれば、$C_A(t)=C_G(t)\cap C_G(y)$.（但、y は $C_G(y)=A$ をみたす元）であり、$t\in Z(A)$ 又は $C_A(t)=B$ のいずれかが成り立つ。従って、

$$|A:C_A(t)| = \begin{cases}|A:B|=n & ,\ \text{or}\\ 1\end{cases}$$

であり、(A,n,π) は先の定理の仮定をみたす。もし $|\pi|>1$ であれば $A=$ nilp となり $n=p^a$ が直ちに出る。

$\pi=\{p\}$ であれば、${}^\exists q\mid n$, $q=$ prime $\neq p$ とすれば

Q を A の Sylow q-subgp, $1 \neq z \in Z(Q)$ とすれば $C_A(z) = B$ or A (graph の形から) が成り立たねばならないが、$q|n$ から $C_A(z) = A$ である。しかし $Z(G) = 1$ ($\because G =$ simple を仮定) から $C_G(z) = A$ となり、これは $|\pi| = \{p\}$ に矛盾する。

② ①のことから、$n_3 = n_1 p_1^{e_1}$

$$n_4 = n_2 q_1^{f_1} \qquad p_1, q_1 = \text{primes}$$

としてよい。更に Burnside の結果により、n_1, n_2 は prime power でない。従って、$\exists p_2 | n_1,\ p_2 \neq q_1$

$$\exists q_2 | n_2,\ q_2 \neq p_1$$

である。さて、この時 $G \ni \forall w$ に対して、$|G : C_G(w)|$ は p_2 が q_2 と互に素になる。このことから Čunihin の結果 (とその Ito による拡張、cf [1]) から、$G =$ not simple が出る。

Camina の定理の証明には、次の補題を用いる。

<u>補題</u>

$$\left.\begin{array}{l} G = \text{a finite gp} \\ H = \text{a subgp of } G \\ n = \text{an integer} \\ \forall x \in H,\ x \notin Z(G) \Rightarrow |G : C_G(x)| = n \end{array}\right\} \Longrightarrow$$

(1) $H/H \cap Z(G)$ は abelian partition を持つ

(2) $x, y \in H$, $[x, y] \in Z(G)$,

$m = |xZ(G)| \neq |yZ(G)| = n'$ ($G/Z(G)$ での order),

$m \nleqq n'$

$\Rightarrow$ $x(H \cap Z(G))$, $y(H \cap Z(G))$ は $H/Z(G) \cap H$ の同じ component に属する。

(3) $x \in H$, $|xZ(G)| \neq$ 素数（かつ $\neq 1$）

$\Rightarrow$ $U/Z(G) \cap H$（但、$U \underset{def}{=} C_H(x)$）は $x(H \cap Z(H))$ の属する component を含む。

<u>補題の証明</u> (1) $x \in H - Z(G)$ に対して $U(x) = C_H(C_G(x))$ とおけば、$U(x)/H \cap Z(G) = C_H(C_G(x))/H \cap Z(G)$ が partition を作ることは、$w \in U(x) \cap U(y)$ ($U(x) \neq U(y)$) から $C_G(w) \geqq \langle C_G(x), C_G(y) \rangle$ が得られ，更に $w \notin Z(G)$ であれば、$|C_G(w)| = |C_G(x)| = |C_G(y)|$ が成り立たねばならないことから $w \in Z(G)$ が得られることから O.K. また、partition が abelian であることは、$C_H(C_G(x))$ が $Z(C_G(x))$ の subgp であることから O.K. である。

(2) $[x, y] \in Z(G)$ から $(xy)^m = x^m y^m [x, y]^{\frac{m(m-1)}{2}}$ が成り立ち、従って、$(xy)^m = y^m [x, y]^{m(m-1)/2}$、従って

$C_G((xy)^m) = C_G(y^m)$ である。$(y^m \notin Z(G))$。更に仮定から、$C_G(xy) = C_G((xy)^m) = C_G(y)$. 従って、$x \in C_G(y)$ であり、$C_G(x) = C_G(y)$ だから O.K. である。

(3) p = prime, $p \mid |x|$ とすれば、$x^p \notin Z(G)$ である。一方、$U(x)$ は abelian だから、$U(x) \leq C_H(x)$ である。今、y が x を mod $Z(G)$ で centralize し、$y \notin Z(G)$ とすれば y は x, x^p のいずれとも mod $Z(G)$ で異なる order を持つ。従って (2) により $y \in U(x)$, $y \in U(x^p)$ のいずれかが成り立つが、$C_G(x) = C_G(x^p)$ であるから $U(x) = U(x^p)$ であり、従って $y \in U(x)$ であり O.K. である。

定理の証明の概略

目標は $|\pi| > 1$ の時に $^\forall x \in G - Z(G)$ に対して $|G : C_G(x)| = n$ をいうことであり、これがいえれば Ito の結果 ([1]) から O.K. である。

(1) $\pi(G) = \pi(G/Z(G))$ と仮定してよい。

(∵ そうでなければ abelian な Sylow gp の直積としてくっつくだけ)

(2) $\pi \leq \pi(G)$ と仮定してよい。

(∵ そうでなければ、G の conj. rank は 1 になるから Ito の結果 [1] から O.K.)

(3) 以下 $|\pi| > 1$ を仮定してよい。

I. $|\pi| > 2$のとき.

$^\exists x \in G - Z(G)$, $|G : C_G(x)| \neq n$ としてよい。

$$x = \underset{\substack{\uparrow\\ p_1\text{-part}}}{x_1}\ \underset{\substack{\uparrow\\ p_2\text{-part}}}{x_2} \cdots \underset{\substack{\uparrow\\ p_r\text{-part}}}{x_r}\ \underset{\substack{\uparrow\\ p'\text{-part}}}{y}$$

(仮定から $^\forall x_i \notin Z(G)$ としてよい ∵ $x_i \neq 1$ としても同じだから)

とする。(但 $\pi = \{p_1, p_2, \cdots, p_r\}$)

$y \notin Z(G)$であれば

$|G : C_G(x_i y)| = |G : C_G(x_i) \cap C_G(y)| = |G : C_G(y)| = n$

(for $^\forall i$) から $C_G(x_i) = C_G(y)$ であり $C_G(x) = C_G(y)$ となり矛盾。$y \in Z(G)$ でも $|G : C_G(x_i x_j)| = |G : C_G(x_i) \cap C_G(x_j)| = n$ (∵ $r > 2$) から $C_G(x_i) = C_G(x_j)$ $^\forall i, j$ であり $C_G(x) = C_G(x_i)$ が出て矛盾。従って以下 $|\pi| = 2$ ($\pi = \{p, q\}$) としてよい。

II. $\pi < \pi(G)$ のとき.

$^\exists x \in G - Z(G)$, $|G : C_G(x)| \neq n$, $x = \underset{p\text{-part}}{x_1}\ \underset{q\text{-part}}{x_2}\ y$

とすれば、I の議論から $y = 1$ と仮定してよい。

$q \in \pi - \pi(G)$ とする. $G/Z(G)$ の Sylow q-subgp の order をq^bとする。$w = q$-elt $\notin Z(G)$とする. この時、$|G : C_G(w)| = n$であり. $C_G(w) \geq \langle w, Z(G) \rangle$ である。従って、$q^b \nmid |G : C_G(w)|$である. 元 $x = x_1 x_2$ について考え

れば、$|G : C_G(x_1)| = n$ であり、$C_G(x_1)$ は v= q-elt $\notin Z(G)$ を含む。今 $q \notin \pi$ から $|G : C_G(x_1 v)| = n$ である。また、$C_G(x_1 v) = C_G(x_1) \cap C_G(v)$ から $C_G(x_1) = C_G(v)$ である。また、$x_2 \in C_G(x_1)$ から $x_2 \in C_G(v)$ であり、従って $v \in C_G(x_2)$、従って $C_G(x_2) = C_G(v)$ である。従って $C_G(x_1) = C_G(x_2) = C_G(x_1 x_2)$ であり、$|G : C_G(x)| = n$ となり、これは矛盾である。従って、以下 $\pi = \pi(G)$ と仮定してよい。

III. $|\pi| = 2$, $n = p^a$, $p \in \pi$ の場合.

x = p-elt $\notin Z(G)$ とする。この時、$|G : C_G(x)| = p^a$ であり

$$G = C_G(x)\,\overset{\text{Sylow } p\text{-subgp of } G}{\underset{\ni x}{P}} \quad \text{となり} \quad \langle\langle x \rangle\rangle \le P$$

x で生成される G の最小の normal subgp

[Cf. Baer, Trans. A.M.S. 1953] が言え、$P \lhd G$ である。更に、P に含まれる G の chief series を考えることにより P が G の hypercenter に含まれることが導びかれ、P は任意の p'-elt と可換である。従って、G は nilpotent となる。

IV $\pi = \{p, q\}$, p, q = distinct primes の場合.
(従って $\pi(G) = \pi = \pi(n)$ でもある。)
この場合、Burnside の結果より、G = solvable である。

$n = p^a q^b$ とする。定理の仮定から直ちに

$$Z(P) = Z(G) \cap P, \qquad Z(Q) = Z(G) \cap Q$$

Gの Sylow p-subgp　　Gの Sylow q-subgp
(いずれも以下 fix する)

が得られる。この時、P, Q は補題の仮定をみたす。従って P, Q に対して補題の結論が成り立つ。更に Hall-Higman の定理 A (p or q が Fermat prime の時は余分な考察をしなければならないが) を用いて、$P/Z(P)$, $Q/Z(Q)$ の exponent がそれぞれ p, q であれば、G の p-length, q-length がそれぞれ 1 であることがわかる。

次にわかることは、$Z(P)$の上にのっている G の chief-factor $B/Z(P)$ で $[G, B] \not\leq Z(G)$ である G の characteristic p-subgp B の存在を仮定してよい。(∵ $A/Z(G)$ が G の $[A, G] \leq Z(G)$ となる chief factor であり p-gp ならば $|C/C_G(x)| = n = p^a q^b$. 一方、$x \in Z_2(P)$ から $|C/C_G(x)| = p^{\varphi}$ となり矛盾. 以下 p, q の対称性から主張は O.K.)

その次にわかることは、Q が $B/Z(P)$ 上に half-transitive に働くことを示すことである。これは G の p-length が 1 の場合とそうでない場合にわけておこなわれる。p-length が 1 であれば、$|G : C_G(B/Z(P))|$ は q^{φ} が導びかれ、更に

$^{\forall}x \in B$, $x \notin Z(P)$ に対して、$C_G(xZ(P))/C_G(x)$ が p-gp となるから、$xZ(P)$は丁度 q^b 個の conjugate を持つことになり O.K. である。p-length が 1 でなければ $P/Z(P)$ の exponent $> p$ であり $^{\exists}y \in P$ s.t. $y^p \notin Z(P)$, としてよい。更に、$|P : C_P(y)| = p^a$ としてよい。さて、補題から、$C_P(C_G(y))$ は abelian であり $C_P(y)$ と等しい。今 $^{\forall}w \in C_G(y)$ に対して、$C_G(w) \geq C_P(y)$ であり，特に $w = q$-elt $\in C_G(y)$，$w \notin Z(G)$ に対して $C_G(w) \geq C_P(y)$ である。従って、$|G : C_G(w)| = p^a q^b$ とあわせて，$|P : C_P(y)| = p^a$ が得られる。従って $C_P(y)$ は $C_G(w)$ の Sylow p-subgp となり，$C_P(w) = C_P(y)$ である。更に $B \triangleleft G$ から $C_B(y) = C_B(w)$ である。ここで $\langle w \rangle \times \langle y \rangle$ は commute するから Thompson の $p \times q$ Lemma により w は B を centralize する。今，R_y を $C_G(y)$ の Sylow q-subgp かつ $R \geq R_y$ を G の Sylow q-subgp とすれば $|R : C_R(B)| = q^b$ である。従って $|Q : C_Q(B)| = q^b$ である。 $^{\forall}x \in B - Z(P)$ に対して，$|Q : C_Q(x)| \leq q^b$ であるが $\geq q^b$ は常に成り立つから，$|Q : C_Q(x)| = q^b$ である。従って主張は O.K. である。

以下の目標は p-gp に q-gp が half-transitive に働らく時の Issac-Passman : Can. J. Math. 18 (1966) による群の分類を用いて、$b=1$, i.e. $n = p^a q$ となるこ

とを示すことである。[以下は伊藤先生の講演でも時間の関係もあり、ほとんどふれられなかったのでこの記録でも略す。詳しくは、Camina の原論文を参照して下さい。] そして $b=1$ がいえれば、次の方針は $O_q(G) > Z(Q)$ の場合が起こらないことを言って、(この場合は、p と q の対称性から $n=pq$ になり比較的容易に終る)、最後に $O_q(G) = Z(Q)$ となった時は、いずれの場合も(これも G の p-length が 1 の場合と >1 の場合にわけ、更び Thompson の補題 Lemma とか Issac-Passman の結果を用いるが) $Q/Z(Q)$ が cyclic となることが導びかれる。これは明らかに矛盾であり、定理の証明は終る。

§3. さて最後の話題は factorizable group についてである。

$$G = C_G(a)\, C_G(b), \quad a \neq 1, \; b \neq 1$$

と表わされる時、G を factorizable と呼ぶ。例えば $G = H \times K$ (H, K は任意の群) は factorizable である。

<u>予想</u> $G =$ factorizable $\Longrightarrow$ $G =$ not simple

が直接証明出来れば非常に望ましい。もし出来ればこれは最初にのべたBurnside の theorem の拡張になっている。何故なら. $|G : C_G(x)| = p^a$, $P =$ a Sylow p subgp of G $\Rightarrow G = C_G(x) \cdot P$ であり $1 \neq y \in Z(P)$ をとれば $C_G(y) \geq P$ であるからである。

factorizable な群の例として次のものがある.

<u>Example 1</u> Affine group

(i) $G = \underbrace{(2, \cdots, 2)}_{n} \cdot GL(n, 2)$

a として $(2, \cdots, 2)$ の1つの involution を, b として singer cycle (order $2^n - 1$ の元) をとればよい。この場合 $\mathrm{Core}(C_G(a)) \neq 1$ ($\mathrm{Core}(C_G(a)) =$ the largest normal subgp of G contained in $C_G(a)$).

(ii) $G = \underbrace{(q, \cdots, q)}_{n} \cdot GL(n, q)$, $q > 2$

この場合 $a = (q, \cdots, q)$ の order q の元, $b =$ singer cycle の factorization $G = C_G(a) C_G(b)$ の他に

$b^* = \begin{pmatrix} \beta & & \\ & \ddots & \\ & & \beta \end{pmatrix} \neq 1$ をとっても $G = C_G(a) C_G(b^*)$ と factorizable である。

<u>Example 2</u>

$$SL(2, q) \ : \ q = \text{odd} > 3$$

S : simple nonabelian gp

をとり.

$G = S \wr SL(2,q) \quad (\overbrace{S \times \cdots \times S}^{SL(2,q)})$ とおく。

a として $SL(2,q)$ の central involution, b として S の involution をとれば、$G = C_G(a)C_G(b)$ である。この場合 $Core(C_G(a)) = Core(C_G(b)) = 1$。

このExample 2はこの問題の難かしさを示すであろう。

以下の目標は次の定理に証明を与えることである。

<u>定理(Ito)</u>

$$\left.\begin{array}{l} G = 4\text{重可移群 on } \Omega = \{1, \cdots, n\} \\ G = \text{factorizable} \\ \quad \text{i. e., } G = C_G(a)C_G(b) \end{array}\right\} \Rightarrow \begin{array}{l} n = 4 \\ G = S_4 \end{array}$$

<u>証明</u> ① 先ずfactorizableのdefから直ちに $[a][b] = m[ab]$ が成りたつ。($\because$ $a^x b^y = a^z b^z$ を言えばよい) ここで $[a]$ は a と共役な元全体の和($\mathbb{Z}$ 上の G の group ring の中での)をあらわす。

② 更に $\chi(a)\chi(b) = \chi(1)\chi(ab)$ for $\forall \chi$: irred character が成り立つ。

$x \in G$ に対して $\alpha(x) = x$ の fixed pts の数,

$\beta(x) = x$ の cycle structure における互換の数、とする。

③ $\alpha(a)\alpha(b) = 0$.

otherwise $a = (\cdot)\cdots(\cdot) \longmapsto$ となり

$C_G(a)$ は not transitive となり、更に $C_G(b)$ も not transitive である。一方 $G = 2$-trans から

$$\alpha = 1_G + \underset{\substack{\uparrow \\ \text{irred char}}}{\chi_0}$$ とかけるが、

$\alpha | C_G(a)$ intransitive から $(\alpha|_{C_G(a)}, 1_{C_G(a)}) > 2$

従って、$\chi_0|_{C_G(a)} = \square\, 1_{C_G(a)} + \cdots \qquad (\square > 0)$

$\chi_0|_{C_G(b)} = \bigcirc\, 1_{C_G(b)} + \cdots \qquad (\bigcirc > 0)$

となり、従って、

$$1_{C_G(a)}^G = 1_G + \square\,\chi_0 + \cdots$$

$$1_{C_G(b)}^G = 1_G + \bigcirc\,\chi_0 + \cdots$$

となり、$(1_{C_G(a)}^G, 1_{C_G(b)}^G) > 1$

一方、$G = C_G(a)C_G(b)$ から $(1_{C_G(a)}^G, 1_{C_G(b)}^G) = 1$

であり、これは矛盾である。

以下、$\alpha(a) = 0$ と仮定してよい。この時、$\alpha = 1_G + \chi_0$

$\chi_0(a) = -1$ である。この時、②より

④ $$-\chi_0(b) = \underset{\substack{\uparrow \\ \text{degree of } \chi_0}}{(n-1)}\chi_0(ab)$$

が成り立つ。従って、

$$\chi_0(b) = 0 = \chi_0(ab)$$
$$\alpha(b) = \alpha(ab) = 1 \quad \text{である。}$$

明らかに、

⑤ $|a|, |b| = prime$ と仮定してよい。

$$a = (\underbrace{\qquad\qquad}_{p})(\underbrace{\qquad\qquad}_{p})(\underbrace{\qquad\qquad}_{p})\cdots\cdots$$
$$b = (1)(\underbrace{\qquad\qquad}_{q})(\underbrace{\qquad\qquad}_{q})(\underbrace{\qquad\qquad}_{q})\cdots\cdots$$

とする。

さて、

$$\chi_{\overset{\circ}{\underset{\circ}{}}} = \frac{(\alpha-1)(\alpha-2)}{2} - \beta$$
$$\chi_{00} = \frac{\alpha(\alpha-3)}{2} + \beta$$

とおく。（これらは G の4重可移性から G の irred. char を与える。）

$$\begin{array}{l|l} \chi_{\overset{\circ}{\underset{\circ}{}}}(a) = 1-\beta(a) & \chi_{\overset{\circ}{\underset{\circ}{}}}(b) = -\beta(b) \\ \chi_{\overset{\circ}{\underset{\circ}{}}}(a) = \beta(a) & \chi_{00}(b) = -1+\beta(b) \end{array}$$

が成り立つ。

さて、Theorem の証明は次のようにして完成される。

(i) $p, q > 2$ ならば

$$\beta(a) = \beta(b) = 0, \quad \alpha(ab) = 1 \quad \text{であり}$$
$$\chi_{\overset{\circ}{\underset{\circ}{}}}(a) = 1,\ \chi_{\overset{\circ}{\underset{\circ}{}}}(b) = 0 \implies \chi_{\overset{\circ}{\underset{\circ}{}}}(ab) = 0 = -\beta(ab)$$
$$\chi_{00}(a) = 0,\ \chi_{00}(b) = -1 \implies \chi_{00}(ab) = 0 = -1+\beta(ab)$$

で矛盾。

(ii) $q=2,\ p>2$ ならば $\beta(b)=\frac{n-1}{2}$ であり

$\chi_{\overset{\circ}{\circ}}(a)=1 \qquad \chi_{\overset{\circ}{\circ}}(b)=-\frac{n-1}{2}$

従って、 $-\frac{n-1}{2}=\frac{(n-1)(n-2)}{2}\chi_{\overset{\circ}{\circ}}(ab)$ から $n=3$ が出て矛盾。

(iii) $p=2,\ q>2$ ならば $\beta(b)=0,\ \beta(a)=\frac{n}{2}$

$\chi_{\circ\circ}(a)=\frac{n}{2}\ ,\ \chi_{\circ\circ}(b)=-1$ から

$-\frac{n}{2}=\frac{n(n-1)}{2}\chi_{\circ\circ}(a)$ から

$n=4$ が出る。 Q.E.D.

なお、次のことも証明されている。

<u>定理 (Ito) [7]</u>

$$\left.\begin{array}{l} G=3\text{-trans} \\ \quad\ \text{degree } n \\ G=\text{factorizable} \end{array}\right\} \Rightarrow \begin{array}{l} n=2 \\ \underbrace{(2,\cdots,2)}_{m} \lhd G \end{array}$$

i.e., $G=(2,\cdots,2)X$

$X = 2\text{-trans}.$

(この場合 $X=GL(m,2)$ と思われるが証明出来ないとのことである。)

なお、次のことも証明されているとのことである。

$$
\left.\begin{array}{l}
G = C_G(a)\,C_G(b) \\
\qquad C_G(b) \geq B = \text{cyclic} \\
G = C_G(a)\,B
\end{array}\right\} \Rightarrow G = \textit{not simple}
$$

方針は $|B| \neq$ prime power としてよいが、この場合 $C_G(a) \cap B = 1$，$C_G(a) =$ maximal in G がいえて、Schur の Th. から G は $C_G(a)$ による coset 上 2 重可移が出て、更に、G が regular normal subgp を持つことが Glauberman などの結果 ($|a| =$ even の場合) ($|a| =$ odd の場合は他の考察) を用いていえるとのことである。[なお、factorizable な 2 重可移群の分類（少なくともそれが regular normal subgp を持つこと）がいえれば望ましいが、これについては、後の松江の代数学分科会での伊藤先生の講演で証明の idea が見つかったことを話された。]

参考文献

A. Camina : [1] Conjugacy classes of finite groups and some theorems of N. Ito, J. London Math. Soc. 6 (1973), 421–426

[2] Finite groups of conjugate rank 2 (to appear)

N. Ito, [1] On finite groups with given conjugate types I,
Nagoya J. Math. 6 (1953), 17-28.
[2] ———, II, Osaka J. Math. 7 (1970), 231-251
[3] ———, III, Math. Zeit. 117 (1970), 267-271
[4] Simple groups of conjugate type rank 4,
J. Algebra 20 (1972), 226-249.
[5] Simple groups of conjugate type rank 5.
J. Math. Kyoto Univ. 13 (1973), 171-190
[6] On factorizable groups, Proc. Symp. Pure
Math. 21 (1971), 77-83.
[7] On factorizable groups (to appear)

M. M. Markel [1] Groups with many conjugate elements
J. Alg. 26 (1973). 69-74.
[2] Thesis (1971) Univ. of Toront